



Guide de l'utilisateur du service IM and Presence sur la plate-forme Cisco Unified Communications Manager, version 9.0(1)

Première publication: 25 Mai 2012

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

LES SPÉCIFICATIONS ET INFORMATIONS RELATIVES AUX PRODUITS PRÉSENTÉS DANS CE MANUEL SONT SUSCEPTIBLES DE MODIFICATIONS SANS PRÉAVIS. TOUTES LES DÉCLARATIONS, INFORMATIONS ET RECOMMANDATIONS FOURNIES DANS CE MANUEL SONT EXACTES À NOTRE CONNAISSANCE, MAIS SONT PRÉSENTÉES SANS GARANTIE D'AUCUNE SORTE, EXPRESSE OU IMPLICITE. LES UTILISATEURS ASSUMENT L'ENTIÈRE RESPONSABILITÉ DE L'APPLICATION DE TOUT PRODUIT.

LA LICENCE DE LOGICIEL ET LA GARANTIE LIMITÉE DU PRODUIT CI-JOINT SONT DÉFINIES DANS LES INFORMATIONS FOURNIES AVEC LE PRODUIT ET SONT INTÉGRÉES AUX PRÉSENTES SOUS CETTE RÉFÉRENCE. SI VOUS NE TROUVEZ PAS LA LICENCE DE LOGICIEL OU LA GARANTIE LIMITÉE, CONTACTEZ VOTRE REPRÉSENTANT CISCO POUR EN OBTENIR UNE COPIE.

L'implémentation par Cisco de la compression d'en-tête TCP est une adaptation d'un programme développé par l'Université de Californie, Berkeley (UCB) dans le cadre de la version du domaine public de l'UCB du système d'exploitation UNIX. Tous droits réservés. Copyright © 1981, Regents of the University of California.

PAR DÉROGATION À TOUTE AUTRE GARANTIE DÉFINIE ICI, TOUS LES FICHIERS DE DOCUMENTATION ET LOGICIELS DE CES FOURNISSEURS SONT FOURNIS "EN L'ÉTAT" AVEC TOUS LEURS DÉFAUTS. CISCO ET LES FOURNISSEURS SUSMENTIONNÉS DÉCLINENT TOUTE GARANTIE EXPLICITE OU IMPLICITE, NOTAMMENT CELLES DE QUALITÉ MARCHANDE, D'APTITUDE À UN BUT PARTICULIER ET DE NON-CONTREFAÇON, AINSI QUE TOUTE GARANTIE EXPLICITE OU IMPLICITE LIÉE A DES NÉGOCIATIONS, À UN USAGE OU À UNE PRATIQUE COMMERCIALE SANS LIMITATION.

EN AUCUN CAS CISCO OU SES FOURNISSEURS NE SAURAIENT ÊTRE TENUS POUR RESPONSABLES DE DOMMAGES INDIRECTS, SPÉCIAUX, CONSÉQUENTS OU ACCIDENTELS, Y COMPRIS ET SANS LIMITATION, LA PERTE DE PROFITS OU LA PERTE OU LES DOMMAGES DE DONNÉES CONSÉCUTIVES À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISER CE MANUEL, MÊME SI CISCO OU SES FOURNISSEURS ONT ÉTÉ AVERTIS DE LA POSSIBILITÉ DE TELS DOMMAGES.

Cisco et le logo Cisco sont des marques de commerce ou des marques déposées de Cisco et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour afficher la liste des marques commerciales Cisco, rendez-vous à l'adresse : <http://www.cisco.com/go/trademarks><http://www.cisco.com/go/trademarks>. Les autres marques de commerce mentionnées sont la propriété de leurs détenteurs respectifs. L'utilisation du mot "partenaire" n'implique aucune relation de partenariat entre Cisco et toute autre entreprise. (1110R)

Les adresses IP (Internet Protocol) utilisées dans ce document sont fictives. Tous les exemples, sorties d'affichage de commandes et chiffres présents dans ce document ne sont donnés qu'à titre indicatif. Toute utilisation d'une adresse IP réelle dans un contenu illustratif serait involontaire et pure coïncidence.

LES SPÉCIFICATIONS ET INFORMATIONS RELATIVES AUX PRODUITS PRÉSENTÉS DANS CE MANUEL SONT SUSCEPTIBLES DE MODIFICATIONS SANS PRÉAVIS. TOUTES LES DÉCLARATIONS, INFORMATIONS ET RECOMMANDATIONS FOURNIES DANS CE MANUEL SONT EXACTES À NOTRE CONNAISSANCE, MAIS SONT PRÉSENTÉES SANS GARANTIE D'AUCUNE SORTE, EXPRESSE OU IMPLICITE. LES UTILISATEURS ASSUMENT L'ENTIÈRE RESPONSABILITÉ DE L'APPLICATION DE TOUT PRODUIT.

LA LICENCE DE LOGICIEL ET LA GARANTIE LIMITÉE DU PRODUIT CI-JOINT SONT DÉFINIES DANS LES INFORMATIONS FOURNIES AVEC LE PRODUIT ET SONT INTÉGRÉES AUX PRÉSENTES SOUS CETTE RÉFÉRENCE. SI VOUS NE TROUVEZ PAS LA LICENCE DE LOGICIEL OU LA GARANTIE LIMITÉE, CONTACTEZ VOTRE REPRÉSENTANT CISCO POUR EN OBTENIR UNE COPIE.

L'implémentation par Cisco de la compression d'en-tête TCP est une adaptation d'un programme développé par l'Université de Californie, Berkeley (UCB) dans le cadre de la version du domaine public de l'UCB du système d'exploitation UNIX. Tous droits réservés. Copyright © 1981, Regents of the University of California.

PAR DÉROGATION À TOUTE AUTRE GARANTIE DÉFINIE ICI, TOUS LES FICHIERS DE DOCUMENTATION ET LOGICIELS DE CES FOURNISSEURS SONT FOURNIS "EN L'ÉTAT" AVEC TOUS LEURS DÉFAUTS. CISCO ET LES FOURNISSEURS SUSMENTIONNÉS DÉCLINENT TOUTE GARANTIE EXPLICITE OU IMPLICITE, NOTAMMENT CELLES DE QUALITÉ MARCHANDE, D'APTITUDE À UN BUT PARTICULIER ET DE NON-CONTREFAÇON, AINSI QUE TOUTE GARANTIE EXPLICITE OU IMPLICITE LIÉE A DES NÉGOCIATIONS, À UN USAGE OU À UNE PRATIQUE COMMERCIALE SANS LIMITATION.

EN AUCUN CAS CISCO OU SES FOURNISSEURS NE SAURAIENT ÊTRE TENUS POUR RESPONSABLES DE DOMMAGES INDIRECTS, SPÉCIAUX, CONSÉQUENTS OU ACCIDENTELS, Y COMPRIS ET SANS LIMITATION, LA PERTE DE PROFITS OU LA PERTE OU LES DOMMAGES DE DONNÉES CONSÉCUTIVES À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISER CE MANUEL, MÊME SI CISCO OU SES FOURNISSEURS ONT ÉTÉ AVERTIS DE LA POSSIBILITÉ DE TELS DOMMAGES.

Cisco et le logo Cisco sont des marques de commerce ou des marques déposées de Cisco et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour afficher la liste des marques commerciales Cisco, rendez-vous à l'adresse : <http://www.cisco.com/go/trademarks><http://www.cisco.com/go/trademarks>. Les autres marques de commerce mentionnées sont la propriété de leurs détenteurs respectifs. L'utilisation du mot "partenaire" n'implique aucune relation de partenariat entre Cisco et toute autre entreprise. (1110R)

Les adresses IP (Internet Protocol) utilisées dans ce document sont fictives. Tous les exemples, sorties d'affichage de commandes et chiffres présents dans ce document ne sont donnés qu'à titre indicatif. Toute utilisation d'une adresse IP réelle dans un contenu illustratif serait involontaire et pure coïncidence.



TABLE DES MATIÈRES

Introduction à l'interface des options utilisateur de Cisco Unified CM IM and Presence 1

Navigateurs pris en charge 1

Se connecter aux options utilisateur de Cisco Unified CM IM and Presence 1

Configuration des politiques de confidentialité 3

Définition de votre politique de confidentialité par défaut 3

Ajout d'utilisateurs internes aux listes d'exceptions autorisées et bloquées 5

Ajout d'utilisateurs externes aux listes d'exceptions autorisées et bloquées 6

Ajout de domaines externes aux listes d'exceptions autorisées et bloquées 7

Organisation de la liste de contacts 9

Ajout de contacts à la liste de contacts 9

Suppression de contacts de la liste de contacts 11

Affichage de la liste de contacts 12

Configuration du temporisateur d'actualisation de la liste de contacts 12

Dépannage de l'interface des options utilisateur de Cisco Unified CM IM and Presence 13

Connexion impossible à l'interface des options utilisateur 13

Déconnexion automatique de l'interface des options utilisateur 13

Options d'accessibilité 15

Accès aux icônes de la fenêtre 15

Accès aux boutons de la fenêtre 15



CHAPITRE 1

Introduction à l'interface des options utilisateur de Cisco Unified CM IM and Presence

- [Navigateurs pris en charge, page 1](#)
- [Se connecter aux options utilisateur de Cisco Unified CM IM and Presence, page 1](#)

Navigateurs pris en charge

L'interface des options utilisateur de Cisco Unified CM IM and Presence prend en charge les navigateurs suivants :

- Microsoft Internet Explorer 6
- Microsoft Internet Explorer 7
- Microsoft Internet Explorer 8
- Firefox 3.x



Remarque

Actuellement, Cisco IM and Presence ne prend en charge ni Safari ni Google Chrome.

Rubriques connexes

[Se connecter aux options utilisateur de Cisco Unified CM IM and Presence, à la page 1](#)

Se connecter aux options utilisateur de Cisco Unified CM IM and Presence

Avant de commencer

Utilisez l'interface des options utilisateur de Cisco Unified CM IM and Presence pour modifier vos paramètres, créer des messages réponses personnalisés et organiser vos contacts.

- Pour pouvoir se connecter à l'interface des options utilisateur de Cisco Unified CM IM and Presence, l'administrateur doit attribuer un groupe "Standard CCM End User" à l'utilisateur.
- Obtenez les informations suivantes auprès de l'administrateur système :
 - L'adresse web des options utilisateur de Cisco Unified CM IM and Presence.
 - Vos identifiant et mot de passe pour accéder aux options utilisateur de Cisco Unified CM IM and Presence.
- Vérifiez que vous utilisez un navigateur pris en charge.

Procédure

- Étape 1** Ouvrez un navigateur Web compatible sur votre ordinateur.
- Étape 2** Saisissez ainsi l'adresse web des options utilisateur de Cisco Unified CM IM and Presence : `http://<serveur IM and Presence>/cupuser`.
- Étape 3** Saisissez vos identifiant et mot de passe pour accéder aux options utilisateur de Cisco Unified CM IM and Presence.
- Étape 4** Saisissez le mot de passe des options utilisateur de Cisco Unified CM IM and Presence fourni par votre administrateur système.
- Étape 5** Sélectionnez **Connex.**
Pour vous déconnecter de l'interface des options utilisateur, sélectionnez **Déconn.** dans le coin supérieur droit de la fenêtre Options utilisateur. Pour des raisons de sécurité, vous serez automatiquement déconnecté des options utilisateur après trente minutes d'inactivité.
-

Rubriques connexes

[Navigateurs pris en charge, à la page 1](#)



CHAPITRE 2

Configuration des politiques de confidentialité

- [Définition de votre politique de confidentialité par défaut, page 3](#)
- [Ajout d'utilisateurs internes aux listes d'exceptions autorisées et bloquées, page 5](#)
- [Ajout d'utilisateurs externes aux listes d'exceptions autorisées et bloquées, page 6](#)
- [Ajout de domaines externes aux listes d'exceptions autorisées et bloquées, page 7](#)

Définition de votre politique de confidentialité par défaut

Les politiques de confidentialité permettent de déterminer quels sont les utilisateurs autorisés à voir votre statut et à vous envoyer des messages instantanés. Cette version de messages instantanés prend en charge la règle de liste de contacts qui stipule que toute personne figurant sur la liste (que vous pouvez surveiller) peut, par défaut, voir votre statut, *à moins que* vous ne refusiez explicitement d'accorder une telle autorisation à cette personne.

Ainsi, les politiques de confidentialité permettent d'autoriser et de bloquer des utilisateurs et des domaines. Les options suivantes vous permettent de configurer la politique de confidentialité, soit en tant que paramètre par défaut au niveau de l'organisation, soit par l'envoi d'une requête spécifique à l'utilisateur.

- **Autoriser** : par défaut, les utilisateurs/domaines peuvent voir votre statut et vous envoyer des messages instantanés, à moins que vous ne les ajoutiez explicitement à votre liste bloquée. Vous pouvez définir la politique de confidentialité Autoriser uniquement pour les domaines et les utilisateurs internes. Cette option n'est *pas* disponible pour les domaines/utilisateurs (fédérés) externes.
- **Bloquer** : les utilisateurs/domaines que vous bloquez ne peuvent pas voir votre statut ni vous envoyer de messages instantanés. Pour eux, vous présentez toujours le statut Non disponible. Vous pouvez définir la politique de confidentialité Bloquer pour les domaines et les utilisateurs (fédérés) internes et externes.
- **Me demander** : la politique de confidentialité Me demander invite les utilisateurs (par l'intermédiaire d'une requête) à bloquer ou à autoriser explicitement l'échange de statuts et de messages instantanés provenant de domaines ou d'utilisateurs spécifiques. L'application client invite l'utilisateur à autoriser ou à rejeter l'abonnement. Vous pouvez définir la politique de confidentialité Me demander uniquement pour les domaines et utilisateurs (fédérés) externes, et seulement si le domaine ou contact externe ne figure *pas* dans la liste autorisée ou la liste bloquée de l'utilisateur.

Procédure

Étape 1 Sélectionnez **Options utilisateur > Politiques de confidentialité**.

Étape 2 Sélectionnez l'une des options suivantes :

Pour...	Procédez comme suit :
<p><i>Autoriser tous les utilisateurs internes</i> à voir votre disponibilité et à vous envoyer des messages instantanés (à l'exception des utilisateurs/domaines internes que vous ajoutez explicitement à votre liste d'exceptions bloquées).</p> <p>Remarque Consultez l'exception à ce paramètre de politique dans la section Conseils relatifs au dépannage de cette rubrique. Cette politique ne permet pas aux utilisateurs externes de voir votre disponibilité.</p>	<ol style="list-style-type: none"> 1 Sélectionnez Autoriser dans le menu déroulant Utilisateurs internes (de votre société/organisation) . 2 (Facultatif) Ajoutez des utilisateurs internes à vos listes d'exceptions bloquées selon les procédures décrites dans ce module. Reportez-vous à la rubrique Que faire ensuite.
<p><i>Empêcher tous les utilisateurs internes</i> de voir votre disponibilité et de vous envoyer des messages instantanés (à l'exception de ceux que vous ajoutez à votre liste d'exceptions autorisées).</p> <p>Remarque Cette politique n'empêche pas les utilisateurs externes de voir votre disponibilité.</p>	<ol style="list-style-type: none"> 1 Sélectionnez Bloquer dans le menu déroulant Utilisateurs internes (de votre société/organisation) . 2 (Facultatif) Ajoutez des utilisateurs internes à votre liste d'exceptions autorisées selon les procédures décrites dans ce module. Reportez-vous à la rubrique Que faire ensuite.
<p><i>Empêcher tous les utilisateurs externes</i> de voir votre disponibilité et de vous envoyer des messages instantanés (à l'exception de ceux que vous ajoutez explicitement à votre liste d'exceptions autorisées).</p> <p>Remarque Cette politique n'empêche pas les utilisateurs internes de voir votre disponibilité.</p>	<ol style="list-style-type: none"> 1 Sélectionnez Bloquer dans le menu déroulant Utilisateurs externes (tous les autres) . 2 (Facultatif) Ajoutez des utilisateurs externes à votre liste d'exceptions autorisées selon les procédures décrites dans ce module. Reportez-vous à la rubrique Que faire ensuite.
<p><i>Inviter tous les utilisateurs</i> (à l'aide d'une requête Me demander) à définir leur propre politique Autoriser/Bloquer pour les utilisateurs externes (à l'exception de ceux que vous ajoutez à votre liste d'exceptions autorisées/bloquées).</p> <p>Remarque Cette politique n'empêche pas les utilisateurs internes de voir votre disponibilité.</p>	<ol style="list-style-type: none"> 1 Sélectionnez Me demander dans le menu déroulant Utilisateurs externes (tous les autres) . 2 (Facultatif) Ajoutez des utilisateurs externes à votre liste d'exceptions autorisées/bloquées selon les procédures décrites dans ce module. Reportez-vous à la rubrique Que faire ensuite.

Étape 3 Sélectionnez **Enregistrer les valeurs par défaut**.

Conseils pour le dépannage

Le serveur IM and Presence autorise automatiquement un utilisateur figurant sur la liste de contacts d'un autre utilisateur à voir son statut. Notez cette exception à la politique *Autoriser tous les utilisateurs internes* : si

vous *désactivez* l'autorisation automatique sur le serveur IM and Presence et si les paramètres par défaut du domaine global et du domaine local sont tous les deux définis par Autoriser, l'utilisateur est invité à approuver ou à rejeter la requête d'abonnement. Il s'agit du scénario Me demander pour le domaine local. Pour plus d'informations sur le paramètre d'autorisation automatique sur le serveur IM and Presence, reportez-vous au *Guide de déploiement du Service IM and Presence sur la plate-forme Cisco Unified Communications Manager* (sur Cisco.com).

Que faire ensuite

- Si vous souhaitez remplacer la politique de confidentialité Autoriser/Bloquer par défaut définie pour les utilisateurs internes/externes au niveau de l'organisation, reportez-vous aux rubriques suivantes qui décrivent la configuration des listes d'exceptions pour les utilisateurs.

Ajout d'utilisateurs internes aux listes d'exceptions autorisées et bloquées

Cette procédure permet de gérer les exceptions à la politique de confidentialité générale sous la forme d'une liste autorisée et d'une liste bloquée. Selon la politique de confidentialité par défaut définie au niveau de l'organisation, vous pouvez modifier la liste autorisée ou la liste bloquée. Ainsi, vous pouvez remplacer le paramétrage de la politique par défaut qui consiste à ajouter des personnes spécifiques de votre organisation à la liste autorisée ou à la liste bloquée.

- La définition de la politique d'autorisation pour des utilisateurs spécifiques permet à ces derniers de voir votre statut et de vous envoyer des messages instantanés, même si la politique générale les bloque.
- La définition de la politique de blocage pour des utilisateurs spécifiques empêche ces derniers de voir le statut et d'échanger des messages instantanés lorsqu'ils utilisent des clients Cisco (Cisco Jabber Version 8), même si la politique générale les y autorise. Les utilisateurs de la liste de contacts sont toujours autorisés, à moins qu'ils ne soient explicitement bloqués dans la liste des exceptions. Notez que certains clients tiers XMPP envoient et reçoivent malgré tout des messages instantanés, quelle que soit la politique que vous avez définie.

Avant de commencer

Définissez votre politique de confidentialité par défaut.

Procédure

Étape 1 Sélectionnez **Options utilisateur > Politiques de confidentialité**.

Étape 2 Dans la fenêtre Politique de confidentialité, dans le cadre Paramètres utilisateur, sélectionnez **Ajouter un utilisateur**.

Étape 3 Effectuez l'une de ces opérations :

- Sélectionnez **Autoriser** pour permettre à l'utilisateur de voir votre disponibilité.
- Sélectionnez **Bloquer** pour empêcher l'utilisateur de voir votre disponibilité.

- Étape 4** Entrez un ID utilisateur valide pour l'utilisateur interne. L'ID utilisateur doit exister sur votre réseau interne au format `<IDutilisateur@domaine>`.
- Étape 5** Sélectionnez **Domaine local**.
- Étape 6** Sélectionnez **Ajouter** pour ajouter l'utilisateur interne au domaine local.

Conseils pour le dépannage

- Les utilisateurs fédérés peuvent ajouter un utilisateur local à l'aide d'un ID d'e-mail ou d'un JID standard. Le choix varie selon que l'administrateur ait activé ou désactivé l'ID d'e-mail pour le domaine.
- Une fois que vous avez **ajouté** un utilisateur à la liste autorisée/bloquée, les détails s'affichent dans le tableau de cette fenêtre. Pour supprimer un utilisateur dans la liste autorisée/bloquée, cochez la case correspondante et sélectionnez **Supprimer la sélection**.

Ajout d'utilisateurs externes aux listes d'exceptions autorisées et bloquées

Cette procédure permet de gérer les exceptions à la politique de confidentialité générale sous la forme d'une liste autorisée et d'une liste bloquée. Selon la politique de confidentialité par défaut définie au niveau de l'organisation, vous pouvez modifier la liste autorisée ou la liste bloquée. Ainsi, vous pouvez remplacer le paramétrage de la politique par défaut qui consiste à ajouter des personnes spécifiques extérieures de votre organisation à la liste autorisée ou à la liste bloquée.

- La définition de la politique d'autorisation pour des utilisateurs spécifiques permet à ces derniers de voir votre statut et de vous envoyer des messages instantanés, même si la politique générale les bloque.
- La définition de la politique de blocage pour des utilisateurs spécifiques empêche ces derniers de voir votre statut et de vous envoyer des messages instantanés, même si la politique générale les y autorise (par l'intermédiaire d'une réponse positive à une requête Me demander).

Avant de commencer

Définissez votre politique de confidentialité par défaut.

Procédure

- Étape 1** Sélectionnez **Options utilisateur > Politiques de confidentialité**.
- Étape 2** Dans la fenêtre Politique de confidentialité, dans le cadre Paramètres utilisateur, sélectionnez **Ajouter un utilisateur**.
- Étape 3** Effectuez l'une de ces opérations :
- Sélectionnez **Autoriser** pour permettre à l'utilisateur de voir votre disponibilité.
 - Sélectionnez **Bloquer** pour empêcher l'utilisateur de voir votre disponibilité.

Étape 4 Entrez un ID utilisateur valide pour l'utilisateur interne. L'ID utilisateur doit exister sur votre réseau interne au format <IDutilisateur@domaine>.

Étape 5 Sélectionnez l'un des domaines dont l'utilisateur fait partie :

- **Domaine fédéré.**
- **Domaine personnalisé** : domaine externe qui ne figure pas sur la liste des domaines fédérés.

Étape 6 Exécutez l'une de ces opérations :

Si vous avez sélectionné...	Procédez comme suit :
Domaine fédéré	Dans la liste déroulante, sélectionnez le domaine pour lequel vous procédez à une fédération.
Domaine personnalisé	Saisissez le domaine pour l'utilisateur. Remarque Par exemple, saisissez "masociété.com".

Étape 7 Sélectionnez **Ajouter**.

Conseils pour le dépannage

Une fois que vous avez **ajouté** un utilisateur à la liste autorisée/bloquée, les détails s'affichent dans le tableau de cette fenêtre. Pour supprimer un utilisateur dans la liste autorisée/bloquée, cochez la case correspondante et sélectionnez **Supprimer la sélection**.

Ajout de domaines externes aux listes d'exceptions autorisées et bloquées

Avant de commencer

Vous pouvez autoriser ou bloquer l'ensemble d'un domaine externe. Si vous bloquez un domaine externe, toute requête de ses utilisateurs visant à consulter votre disponibilité sera refusée, à condition que vous n'ayez pas ajouté ces utilisateurs externes à votre liste autorisée.

Procédure

Étape 1 Sélectionnez **Options utilisateur > Politiques de confidentialité**.

Étape 2 Dans la fenêtre Politique de confidentialité, dans le cadre Paramètres utilisateur, sélectionnez **Ajouter un domaine**.

Étape 3 Effectuez l'une de ces opérations :

- Sélectionnez **Autoriser** pour permettre à l'utilisateur de voir votre disponibilité.
- Sélectionnez **Bloquer** pour empêcher l'utilisateur de voir votre disponibilité.

Étape 4 Sélectionnez l'un de ces domaines à autoriser ou à bloquer :

- **Domaine fédéré**
- **Domaine personnalisé** : domaine externe qui ne figure pas sur la liste des domaines fédérés.

Étape 5 Exécutez l'une de ces opérations :

Si vous avez sélectionné...	Procédez comme suit :
Domaine fédéré	Dans la liste déroulante, sélectionnez le domaine pour lequel vous procédez à une fédération.
Domaine personnalisé	Saisissez le domaine pour l'utilisateur. Remarque Par exemple, saisissez "masociété.com".

Étape 6 Sélectionnez **Ajouter**.

Conseils pour le dépannage

Une fois que vous avez **ajouté** un domaine à la liste autorisée/bloquée, les détails s'affichent dans le tableau de cette fenêtre. Pour supprimer un domaine dans la liste autorisée/bloquée, cochez la case correspondante et sélectionnez **Supprimer la sélection**.



CHAPITRE 3

Organisation de la liste de contacts

- [Ajout de contacts à la liste de contacts, page 9](#)
- [Suppression de contacts de la liste de contacts, page 11](#)
- [Affichage de la liste de contacts, page 12](#)
- [Configuration du temporisateur d'actualisation de la liste de contacts, page 12](#)

Ajout de contacts à la liste de contacts

Avant de commencer

- L'administrateur système définit le nombre de contacts, inférieur à 100 que peut contenir votre liste. Adressez-vous à lui pour connaître le nombre de contacts maximum défini pour votre téléphone.
- Pour ajouter un contact externe vous pouvez, soit sélectionner un domaine externe, soit configurer un domaine personnalisé pour les utilisateurs qui ne font pas partie de votre organisation.
- Les utilisateurs internes et externes de la liste de contacts sont des exceptions aux politiques internes et externes. Les utilisateurs de la liste de contacts sont toujours autorisés, à moins qu'ils ne soient explicitement bloqués dans la liste des exceptions.
- Dans l'application de votre messagerie instantanée, vous pouvez ajouter des contacts dont vous ne voyez pas le statut. Par exemple, vous pouvez ajouter des personnes que vous souhaitez simplement pouvoir appeler depuis la liste de contacts de l'application. Ces types de contacts ne sont pas visibles dans la liste de contacts de l'interface **Options utilisateur**.
- Si vous apportez des modifications à la liste de contacts (ajout, suppression ou modification), ces changements sont automatiquement pris en compte au niveau des clients Cisco (pour tous les utilisateurs connectés).

Procédure

Étape 1 Sélectionnez **Options utilisateur > Contacts**.

Étape 2 Sélectionnez **Ajouter un nouveau**.

Étape 3 Sélectionnez l'une des options suivantes :

Si le contact que vous souhaitez ajouter est...	Procédez comme suit :
Interne - utilisateur qui appartient à votre domaine local (en général, la société ou l'organisation)	<ol style="list-style-type: none"> 1 Dans le champ Contact, indiquez l'ID utilisateur du contact fédéré que vous souhaitez ajouter. 2 Sélectionnez Sélectionner dans la liste de domaines. 3 Dans le menu Domaine, sélectionnez un domaine interne (local). 4 Vous pouvez également saisir un nom alternatif pour l'utilisateur si vous souhaitez afficher un surnom sur son ordinateur. <p>Remarque Vous ne pouvez pas ajouter des utilisateurs ou des domaines qui sont déjà bloqués par l'administrateur. La politique de confidentialité de l'organisation doit être définie de façon à autoriser le domaine externe ou des utilisateurs spécifiques de ce domaine à voir votre statut et à vous envoyer des messages instantanés.</p>

Si le contact que vous souhaitez ajouter est...	Procédez comme suit :
Externe : utilisateur qui ne fait pas partie de votre domaine local (en général, la société ou l'organisation)	<p>Effectuez l'une des opérations suivantes :</p> <ol style="list-style-type: none"> 1 Dans le champ Contact, indiquez l'ID utilisateur du contact fédéré que vous souhaitez ajouter. 2 Sélectionnez Sélectionnez dans la liste de domaines. <ul style="list-style-type: none"> • Dans le menu Domaine, sélectionnez un domaine externe. 3 Sélectionnez Saisir un domaine personnalisé. <ul style="list-style-type: none"> • Indiquez le domaine personnalisé pour les contacts qui ne font pas partie de votre organisation. <p>Remarque Vous ne pouvez pas ajouter des utilisateurs ou des domaines qui sont déjà bloqués par l'administrateur. La politique de confidentialité de l'organisation doit être définie de façon à autoriser le domaine externe ou des utilisateurs spécifiques de ce domaine à voir votre statut et à vous envoyer des messages instantanés.</p>

Étape 4 (facultatif) Saisissez un nom alternatif (surnom) pour le contact.

Étape 5 Sélectionnez **Enregistrer**.

Conseils pour le dépannage

Vous ne pouvez avoir qu'un seul nom alternatif (surnom) par contact. Si vous saisissez également un nom alternatif pour un contact, celui-ci s'affiche pour les clients Cisco, mais pas nécessairement pour les clients tiers XMPP. Si vous mettez à jour le nom d'un contact, cette modification se répercute dans la liste de contacts sur Cisco Jabber, ainsi que dans tous vos groupes de contacts.

Suppression de contacts de la liste de contacts

Procédure

Étape 1 Sélectionnez **Options utilisateur > Contacts**.

Étape 2 Sélectionnez **Rechercher**.

Étape 3 Effectuez l'une de ces opérations :

Pour...	Procédez comme suit :
Supprimer tous vos contacts	Sélectionnez Tout sélectionner .
Supprimer les contacts sélectionnés	Cochez la case près du nom du contact à supprimer.

Étape 4 Sélectionnez **Supprimer la sélection**.

Étape 5 Sélectionnez **OK**.

Conseils pour le dépannage

La suppression d'un contact peut prendre du temps, car cela implique des opérations au niveau de la base de données. Un message s'affiche dans l'interface utilisateur et indique : "Une récente mise à jour effectuée sur votre liste de contacts n'est pas encore entrée en vigueur. Elle sera traitée très prochainement." Si vous actualisez la page, la liste de contacts mise à jour s'affiche.

Affichage de la liste de contacts

Procédure

Étape 1 Sélectionnez **Options utilisateur > Contacts**.

Étape 2 Sélectionnez **Rechercher**.

Configuration du temporisateur d'actualisation de la liste de contacts

Vous pouvez modifier la fréquence d'actualisation de la liste de contacts sur votre téléphone.

Procédure

Étape 1 Sélectionnez **Options utilisateur > Préférences**.

Étape 2 Saisissez une valeur (en secondes) comprise entre 7 et 3 600 dans le champ **Intervalle d'actualisation de l'écran du téléphone**. La valeur par défaut est 30 secondes.

Étape 3 Sélectionnez **Enregistrer**.



CHAPITRE 4

Dépannage de l'interface des options utilisateur de Cisco Unified CM IM and Presence

- [Connexion impossible à l'interface des options utilisateur, page 13](#)
- [Déconnexion automatique de l'interface des options utilisateur, page 13](#)

Connexion impossible à l'interface des options utilisateur

Problème J'accède à la bonne page Web **Options utilisateur**, mais je ne parviens pas à me connecter à l'aide de mon nom d'utilisateur et de mon mot de passe.

Solution Vérifiez auprès de l'administrateur système que vous utilisez le bon lien pour les pages Web **Options utilisateur**, mais aussi que le nom d'utilisateur et le mot de passe que vous saisissez sont corrects. Vérifiez également que vous êtes enregistré en tant que titulaire d'une licence d'utilisation et que vous disposez de l'accès affecté aux pages Web **Options utilisateur**.

Déconnexion automatique de l'interface des options utilisateur

Problème Je dois à nouveau saisir mes nom d'utilisateur et mot de passe pour accéder à l'interface des options utilisateur.

Solution Pour plus de sécurité, les pages Web Options utilisateur vous déconnectent automatiquement après trente minutes d'inactivité.



CHAPITRE 5

Options d'accessibilité

- [Accès aux icônes de la fenêtre, page 15](#)
- [Accès aux boutons de la fenêtre, page 15](#)

Accès aux icônes de la fenêtre

Les options utilisateur de Cisco Unified CM IM and Presence propose une fonctionnalité qui vous permet d'accéder aux icônes de la fenêtre sans utiliser la souris. Vous pouvez effectuer cette procédure depuis n'importe quel endroit de la fenêtre, ce qui vous évite de faire défiler plusieurs champs.

Dans Cisco IM and Presence, les icônes s'affichent dans la partie supérieure de nombreuses fenêtres, par exemple l'icône d'un disque pour Enregistrer ou un signe plus (+) pour Ajouter, etc.

Procédure

- Étape 1** Appuyez sur ALT, appuyez sur 1, puis appuyez sur Tab.
- Étape 2** Le curseur affiche en surbrillance la première icône à gauche. Appuyez de nouveau sur Tab pour passer à l'icône suivante.
- Étape 3** Appuyez sur Entrée pour exécuter la fonction de l'icône.
-

Accès aux boutons de la fenêtre

Les options utilisateur de Cisco Unified CM IM and Presence propose une fonctionnalité qui vous permet d'accéder aux icônes de la fenêtre sans utiliser la souris. Vous pouvez effectuer cette procédure depuis n'importe quel endroit de la fenêtre, ce qui vous évite de faire défiler plusieurs champs.

Dans Cisco IM and Presence, les boutons s'affichent dans la partie supérieure de nombreuses fenêtres, par exemple le bouton Enregistrer, le bouton Ajouter, etc.

Procédure

- Étape 1** Appuyez sur ALT, appuyez sur 2, puis appuyez sur Tab.
- Étape 2** Le curseur affiche en surbrillance le premier bouton à gauche. Appuyez de nouveau sur Tab pour passer au bouton suivant.
- Étape 3** Appuyez sur Entrée pour exécuter la fonction du bouton.
-